PTH:VAZ
F. #2021R00911

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A SAMSUNG GALAXY CELLULAR TELEPHONE ASSOCIATED WITH IMEI NUMBER 355369106024896 AND CALL NUMBER (347) 768-6515 AND OF A SAMSUNG GALAXY TAB E TABLET, CURRENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION IN THE EASTERN DISTRICT OF NEW YORK	**APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES** Case No. 21-MJ-1158

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, MICHAEL BUSCEMI, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of properties—two electronic devices—that are currently in the possession of the Federal Bureau of Investigation ("FBI") in the Eastern District of New York, as well as the extraction from those properties of electronically stored information ("ESI") described in Attachment B.

2. I have been a Special Agent with the FBI since 2015. Accordingly, I am a "federal law enforcement officer" within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure—that is, a government agent engaged in enforcing the criminal laws and duly authorized by Attorney General to request a search warrant.

3. Since September 2019, I have been assigned to the Child Exploitation and Human Trafficking Task Force. I have investigated numerous violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases, reviewed hundreds of thousands of photographs depicting children being sexually exploited by adults, and executed warrants to search premises, electronic communications, and social media accounts used to facilitate child exploitation offenses.[1] Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

4. I base this affidavit upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement personnel and other individuals, and my training and experience concerning the use of electronic devices in criminal activity and the forensic analysis of ESI.

5. Because I am submitting this affidavit for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during my investigation.

[1] For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit: The terms "minor," "sexually explicit conduct," and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8), in pertinent part, as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ." See also generally Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of definitions set forth in 18 U.S.C. 2256(8)).

6. In this affidavit, I report only in substance and part the contents of documents and the actions, statements, and conversations of others.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The properties to be searched are a Samsung Galaxy cellular telephone associated with International Mobile Equipment Identity ("IMEI") number 355369106024896 and call number (347) 768-6515 and a Samsung Galaxy Tab E tablet (together, the "DEVICES"). The DEVICES are currently in the custody of the FBI in the Eastern District of New York.

8. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying ESI particularly described in Attachment B.

9. The DEVICES belong to Jed Johnson, who is being investigated in connection with violations of Title 18, United States Code, Sections 2252(a)(2) and (b)(1) and 2252A(a)(2)(A) and (b)(1) (receipt of child pornography) and 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) (the "Subject Offenses").

10. On September 29, 2021, the Honorable Lois Bloom, United States Magistrate Judge, signed a Complaint charging Johnson with one count of possession of child pornography, in violation of § 2252(a)(4)(B). See Complaint, United States v. Johnson, No. 21-MJ-1110 (LB) (E.D.N.Y. filed Sept. 29, 2021).

PROBABLE CAUSE

11. On or about June 22, 2020, Google LLC ("Google") identified the e-mail address johnsonjedi2@gmail.com—a Gmail e-mail account later registered to Johnson (the

"Subject Account")—as containing 26 images and one video of child pornography. Ten of the images depicted a prepubescent minor, and 17 of the images depicted a pubescent minor.

12. Google alerted the National Center for Missing and Exploited Children, and I began an investigation into Johnson. I reviewed all 26 images and one video, and each of the files contained child pornography.

13. In response to a July 8, 2020, administrative subpoena, Google advised law enforcement that the Subject Account was accessed by an electronic device associated with T-Mobile US, Inc. ("T-Mobile"). In response to a separate July 8, 2020, administrative subpoena, T-Mobile advised law enforcement that the subscriber of the T-Mobile electronic device was Johnson.

14. On March 2, 2021, the Honorable Vera M. Scanlon, United States Magistrate Judge, signed a search warrant authorizing the recovery from the Subject Account of ESI related to violations of § 2252(a)(2) (receipt of child pornography). Pursuant to the search warrant, I reviewed certain ESI recovered from the Subject Account and confirmed that the Subject Account contained multiple images and videos of child pornography.

15. On September 29, 2021, law-enforcement agents and I visited Johnson at his residence in Queens, New York. After Johnson answered the front door, we asked him whether he was the user of the Subject Account. Johnson said he was in fact the user.

16. Law-enforcement agents asked Johnson whether he would authorize them to review his cellular phone, and whether he had any other electronic devices in his residence. Johnson said he had a cellular phone and a tablet—the DEVICES described above. Johnson provided consent to a search of the DEVICES.

17. Pursuant to Johnson's consent, I reviewed the DEVICES and confirmed that each one contained images of child pornography, including images depicting infants. The images depicted, among other things:

a. a newborn infant laying with an erect penis by the infant's mouth;

b. a blonde prepubescent girl of no more than six years of age facing the camera with her legs spread and genitals exposed; and

c. a prepubescent girl of no more than seven years of age with her legs over her head and genitals exposed.

18. During my search of the DEVICES, Johnson was not handcuffed or otherwise detained. Although he was not advised of his rights under Miranda v. Arizona, 384 U.S. 436 (1966), Johnson made voluntary statements to law-enforcement agents before he was handcuffed. Johnson stated that he searched for and downloaded images of child pornography from the Internet onto his cellular phone and tablet.

19. Since that time, the DEVICES have remained in my custody. In my training and experience, I know that the DEVICE has been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as it was when the DEVICES first came into the possession of the FBI.

20. Based on the investigation to date, there is evidence that Johnson used the DEVICES to download, possess, and view child pornography. Based on my consent search of the DEVICES and Johnson's voluntary statements (see ¶¶ 16-18), I submit that there is probable cause to conclude that information stored on the DEVICES will include evidence, fruits, and instrumentalities of the Subject Offenses.

21. Although Johnson consented to a search of the DEVICES (see ¶ 16), I am requesting a search warrant out of an abundance of caution.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. A wireless telephone sends signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include Global Positioning System ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory

cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS-navigation device uses GPS to display its current location. It often contains records the locations where it has been. Some GPS-navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. GPS consists of twenty-four NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant ("PDA") is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Because of the Internet's structure, connections between devices on the Internet often cross state and international borders, even when the devices are communicating with each other in the same state.

23. Based on my training, experience, and research, I know that the DEVICES have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS-navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the properties.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my training and experience investigating sexual offenses involving children, I know that child pornography collectors typically store and retain their collection of child pornography for extended periods of time. Child pornography is not readily

available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through Internet use.

25. Based on my training and experience, images viewed via the Internet may still be found in the DEVICES even if deleted. Moreover, even when files have been deleted, they can still be forensically recovered months or years later from the DEVICES. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear. Rather, that data remain on the storage medium until they are overwritten by new data.

26. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contains evidence or fruits of the charges and conduct described above. Such techniques include (but are not limited to):

a. Surveying directories or folders and the individual files they contain;

b. Conducting a file-by-file review by "opening" or reading the first few "pages" of such files to determine their precise contents;

c. "Scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

d. Performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation.

27. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only ESI that might serve as direct evidence of the crimes

described on the warrant, but also forensic evidence that establishes how the DEVICES was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact ESI on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, finding evidence of how an electronic device was used, the purpose of its use, who used it, and when sometimes requires establishing that a particular thing is not present on a storage medium.

28. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I am applying would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques—including but not limited to computer-assisted scans of the entire medium—that might expose many parts of the DEVICES to human inspection to determine whether it is or contains evidence described by the warrant.

29. Manner of execution. Because this warrant seeks permission only to examine devices already in my possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICES described in Attachment A to seek and extract the items described in Attachment B.

Respectfully submitted,

Michael Buscemi
Special Agent
Federal Bureau of Investigation

Sworn to before me by reliable electronic means on October 12, 2021:

HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A SAMSUNG GALAXY CELLULAR TELEPHONE ASSOCIATED WITH IMEI NUMBER 355369106024896 AND CALL NUMBER (347) 768-6515 AND OF A SAMSUNG GALAXY TAB E TABLET, CURRENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION IN THE EASTERN DISTRICT OF NEW YORK

Case No. 21-MJ-1158

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A (incorporated by reference).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B (incorporated by reference).

YOU ARE COMMANDED to execute this warrant on or before October 24, 2021 *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 10/12/21 4:30 PM

Judge's signature

City and state: Brooklyn, New York

Hon. Sanket J. Bulsara U.S.M.J.
Printed name and title

Return

Case No.: 21-MJ-1158	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The properties to be searched are a Samsung Galaxy cellular telephone associated with International Mobile Equipment Identity number 355369106024896 and call number (347) 768-6515 and a Samsung Galaxy Tab E tablet (together, the "DEVICES"). The DEVICES are currently in the custody of the Federal Bureau of Investigation in the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records and information on the electronic devices described in Attachment A (the "DEVICES"), that relate to violations of Title 18, United States Code, Sections 2252 and 2252A (the "Subject Offenses") and involve Jed Johnson from June 1, 2020, to the present, including:

1. Images of child pornography and files containing images of child pornography and records, images, information, or correspondence pertaining to the possession, access with intent to view, receipt, and distribution of sexually explicit material relating to children, in violation of the Subject Offenses, in any form wherever they may be stored or found;

2. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

4. Records, information and correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution, and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including:

a. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

b. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce, including by United States mail or by computer, of any visual depiction of minors.

5. Billing and payment records, including records from credit card companies, PayPal, and other electronic payment services, reflecting access to websites pertaining to the Subject Offenses;

6. Address books, names, lists of names, and addresses of individuals believed to be minors;

7. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors;

8. Any and all records, documents, invoices, and materials that concern any Internet accounts used to possess, receive, or distribute child pornography and/or to engage in violations of the Subject Offenses;

9. Evidence of user attribution showing who used or owned the DEVICES at the time of the Subject Offenses, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

10. Records evidencing the use of the DEVICES' Internet Protocol ("IP") addresses to communicate with co-conspirators of the Subject Offenses, including:

a. Records of IP addresses used; and

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as media that can store data) in the DEVICES and any photographic form.

This warrant authorizes the examination of the DEVICES, consistent with the warrant, to locate the evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the law enforcement agents may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.